

State Representative
JEFF MORRIS

P.O. Box 40600
Olympia, WA 98504-0600



Printed on recycled paper

**Consumer
Protection
Newsletter**

**Protecting consumers
against online fraud
and identity theft**

PRESORTED
STANDARD
U. S. POSTAGE PAID
Washington State
Department of Printing



It's an online world

About 137 million Americans use the internet, a number that continues to increase according to Pew Internet research. Most of us go online to send email, but a growing number rely on the Internet to buy products, bank online and pay bills. A great concern among all users is the security of personal information we transmit on the web.

This year, I strengthened Washington State's consumer protection laws by passing measures that are tough on those who commit computer crimes. This newsletter outlines the laws we passed this year and details tips you can take to protect yourself. I believe that educating ourselves against these dangers is the first line of defense for protecting our personal information.

**Consumer
Protection
Newsletter**

**Protecting consumers
against online fraud
and identity theft**



State Representative

JEFF MORRIS

40th District • November 2005

*Chair of the Technology, Energy and
Communications Committee*

Growth of online dangers

Gone are the days when we only had to be wary of opening file attachments. Now, a simple click can get us in trouble. Spyware and phishing are relatively new terms consumers should know about to stay safe online.

What is spyware?

Spyware is a problem that affects everyone who uses the web. These are malicious programs that install themselves on computers to monitor, collect and transmit personally identifiable information without our knowledge or consent.

Spyware programs are not easy to identify or remove and can cause problems ranging from unwanted advertisements to viruses to identity theft. You can unknowingly get spyware just by installing software or visiting a web site.



What is phishing?

Phishing is the result of scammers turning to the internet to commit fraud. Phishing occurs when a fraudulent email or website asks for your personal information, often times to update billing or account information. For example, you might receive an email that appears to be from a familiar business or organization such as a bank or online retailer. The fraudulent email contains a link

to a "fake" website that uses actual trademarks and graphics from a legitimate business. The website asks the user to input personal information (such as your credit card number) and sends the data to scammers, not the legitimate company.

One in three internet users has been a victim of phishing according to Pew Internet research and can result in substantial financial losses. Computer users should be especially wary of unfamiliar charities asking for disaster relief funds.

Popular phishing scams solicit:

- donations for hurricane or tsunami relief
- account information from a bank or online retailer
- personal information to claim a lottery or sweepstakes

Washington laws crack down on online fraud

Spyware

Spyware is more than just an inconvenience. It reduces computer performance and costs money to remove using anti-spyware programs.

Under legislation I sponsored, consumers in Washington State can now take appropriate legal action against spyware purveyors. We're fighting back by enabling the state Attorney General and businesses to seek damages up to \$100,000 per violation. In addition, a court may choose to increase damages up to three times the amount of the award.



Phishing

Phishing is a serious crime that can lead to identity theft. I co-sponsored legislation that creates penalties for anyone trying to get personal information using fraudulent emails or websites. It enables consumers or the Attorney General to seek damages up to \$500 per violation or the amount of actual damages. Internet service providers who are victims may seek up to \$5,000 or actual damages, and the court can increase the fines by up to three times the amount.



Tips to avoid phishing and spyware on the Internet

Avoid phishing scams

- Be suspicious of emails that ask for personal information.
- Don't click on the link in the email; instead contact the company directly via telephone or a website you trust.
- Submit sensitive information only on secure websites of trusted companies.

Prevent spyware from being installed

- Avoid clicking on pop-up windows.
- Install anti-spyware software.
- Do not download programs from untrustworthy websites.

Identity theft

Washington State ranks eighth in the nation for identity theft per capita. To help curtail damages from identity theft, we approved a new "security freeze" law this year. If you're a victim of identity theft, you can request a security freeze on your credit file. This will restrict potential creditors from obtaining your credit history and in most cases, prevent additional credit from being issued in your name.

How to protect yourself against identity theft

- Do not give personal information to strangers via phone, internet or mail.
- Protect your mail, don't leave it in the mailbox for prolonged periods.
- Don't carry your Social Security card.
- Use a shredder to safeguard personal documents.

Resources

Washington State Office
of the Attorney General:
www.atg.wa.gov/
1-800-551-4636

Federal Trade Commission:
www.consumer.gov/idtheft/
1-877-IDTHEFT

State Representative

JEFF MORRIS

1330 A South Second Street, Ste. 100
Mount Vernon, WA 98273
(360) 428-1022

Email: morris.jeff@leg.wa.gov

Website: <http://hdc.leg.wa.gov/members/morris>